PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-298174
(43)Date of publication of application : 12.11.1993

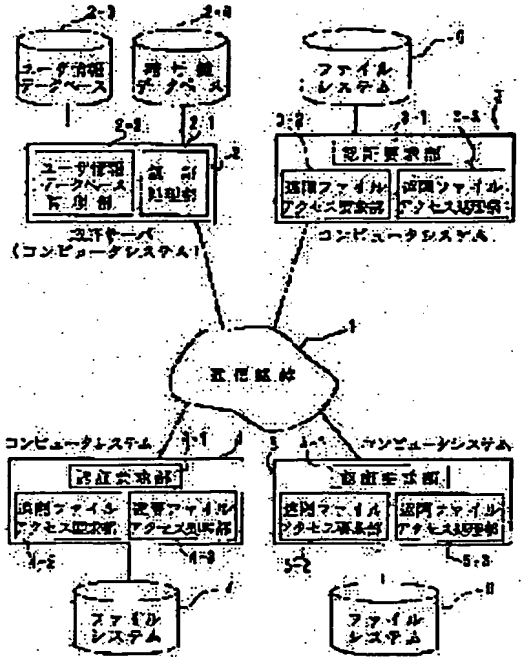
(51)Int.Cl. G06F 12/00
G06F 12/00
G06F 13/00

(21)Application number : 04-101355
(22)Date of filing : 21.04.1992

(71)Applicant : TOSHIBA CORP
(72)Inventor : NUKUI HARUMI

(54) REMOTE FILE ACCESS SYSTEM

(57)Abstract:
PURPOSE: To improve the justification and safety of a file access.
CONSTITUTION: A remote file access request part 3-2 of a computer system 3 to be a remote file access request origin ciphers the authenticated certificate and the access request list acquired by the authentication server (computer system) 2 by a self-decoding key, prepares an access request packet by adding user identification information to the ciphered information, further ciphers it by the ciphering key of an access request destination computer system, and performs the access request of a remote file. A remote file access processing part 4-3 of a computer system 4 to be a remote file access request destination decodes the ciphered access request packet by the self-decoding key, acquires the ciphering key of a user from the authentication server 2 based on the user identification information obtained by further decoding, decodes the authenticated certificate and the access request list and performs the authentication of the user and the processing for the acceptance and rejection of the remote file access.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平５－２９８１７４

(43)公開日　平成５年（１９９３）１１月１２日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ１	技術表示箇所
Ｇ０６Ｆ 12/00	545	Ｆ 8526-5B		
	537	Ｈ 8526-5B		
13/00	351	Ｅ 7368-5B		

審査請求　未請求　請求項の数１　（全６頁）

(21)出願番号　特願平４－１０１３５５

(22)出願日　平成４年（１９９２）４月２１日

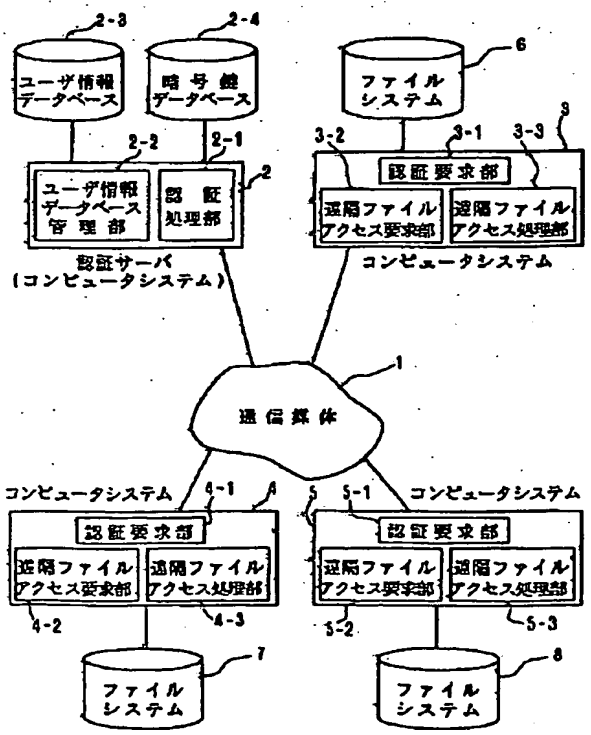
(71)出願人　０００００３０７８
株式会社東芝
神奈川県川崎市幸区堀川町７２番地

(72)発明者　貫井　春美
神奈川県川崎市幸区柳町７０　株式会社東芝柳町工場内

(74)代理人　弁理士　木村　高久

(54)【発明の名称】遠隔ファイルアクセスシステム

(57)【要約】
【目的】ファイルアクセスの正当性と安全性を向上する。
【構成】遠隔ファイルアクセス要求元のコンピュータシステム３の遠隔ファイルアクセス要求部３－２は、認証サーバ２から取得した認証済証明書とアクセス要求リストを自己の復号鍵で暗号化し、該暗号化された情報にユーザ識別情報を付加してアクセス要求パケットを作成し、さらにアクセス要求先コンピュータシステムの暗号鍵で暗号化し、遠隔ファイルのアクセス要求を行い、遠隔ファイルアクセス要求先のコンピュータシステム４の遠隔ファイルアクセス処理部４－３は、暗号化されたアクセス要求パケットを自己の復号鍵で復号化し、さらに復号して得られたユーザ識別情報をもとに認証サーバ２からユーザの暗号鍵を取得し、認証済証明書およびアクセス要求リストを復号し、ユーザの認証および遠隔ファイルアクセス許否の処理を行う。



1

【特許請求の範囲】

【請求項１】複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記複数のコンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、

遠隔ファイルアクセス要求元のコンピュータシステムは、前記認証済証明書とファイルアクセス要求リストを利用者固有の利用者識別情報をもとに暗号化し、該暗号化された情報と利用者識別情報をさらに前記特定のコンピュータシステムから取得したアクセス要求先コンピュータシステムの情報をもとに暗号化し、該暗号化された情報により前記遠隔ファイルのアクセス要求を行う遠隔ファイルアクセス要求手段を有し、

遠隔ファイルアクセス要求先のコンピュータシステムは、前記遠隔ファイルのアクセス要求を自コンピュータシステムがもつ情報により復号して利用者識別情報を得て、さらに該利用者識別情報をもとに暗号化されている前記認証済証明書とファイルアクセス要求リストを復号して利用者の認証および遠隔ファイルアクセス許否の処理を行う遠隔ファイルアクセス処理手段を有して、

相互に認証を行うことを特徴とする遠隔ファイルアクセスシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、任意の通信媒体を介して接続された複数のコンピュータシステムから構成されるネットワークシステム上の遠隔ファイルシステムをアクセスする遠隔ファイルアクセスシステムに関する。

【０００２】

【従来の技術】従来、複数のコンピュータシステムが任意に通信媒体を介して接続された分散環境においては、特定のコンピュータである認証サーバにより利用開始手続が行われ、正しいユーザと判断された時に、認証済証明書が発行され、さらに、その後この認証済証明書を再度認証サーバに提出し、サービス利用のための証明書を得ることによって利用可能になるという手続が行われていた。

【０００３】これに対し、遠隔ノードのコンピュータシステムに存在する遠隔ファイルシステムをアクセスすることができる遠隔ファイルアクセスシステムにおいては、利用者識別子とファイル保護情報の組合せにより、遠隔ファイルアクセスの可否を判断するという単一ノード内と同様な一方的ファイルアクセス形態をとっていた。

【０００４】このため、遠隔ノードのコンピュータシステムからファイルアクセスを要求した利用者が、本来の利用者識別子を所有する利用者であるという保証はなく、不正にアクセスされる可能性があるという問題点があった。

2

【０００５】

【発明が解決しようとする課題】前述したように、複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記コンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、前記認証済証明書による要求元から要求先への一方向の認証であったため、遠隔のコンピュータシステムからファイルアクセスを要求した利用者が、本来の利用者識別子を所有する利用者であるという保証はなく、不正にアクセスされる可能性があるという問題点があった。

【０００６】そこで、本発明は、かかる問題点を除去し、ファイルアクセスの正当性と安全性を向上した遠隔ファイルアクセスシステムを提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明は、複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記複数のコンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、遠隔ファイルアクセス要求元のコンピュータシステムは、前記認証済証明書とファイルアクセス要求リストを利用者固有の利用者識別情報をもとに暗号化し、該暗号化された情報と利用者識別情報をさらに前記特定のコンピュータシステムから取得したアクセス要求先コンピュータシステムの情報をもとに暗号化し、該暗号化された情報により前記遠隔ファイルのアクセス要求を行う遠隔ファイルアクセス要求手段を有し、遠隔ファイルアクセス要求先のコンピュータシステムは、前記遠隔ファイルのアクセス要求を自コンピュータシステムがもつ情報により復号して利用者識別情報を得て、さらに該利用者識別情報をもとに暗号化されている前記認証済証明書とファイルアクセス要求リストを復号して利用者の認証および遠隔ファイルアクセス許否の処理を行う遠隔ファイルアクセス処理手段を有して、相互に認証を行うことを特徴とする遠隔ファイルアクセスシステム。

【０００８】

【作用】本発明は、複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記複数のコンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、遠隔ファイルアクセス要求手段は、遠隔ファイルア

クセス要求元のコンピュータシステムは、前記認証済証明書とファイルアクセス要求リストを利用者固有の利用者識別情報をもとに暗号化し、該暗号化された情報と利用者識別情報をさらに前記特定のコンピュータシステムから取得したアクセス要求先コンピュータシステムの情報をもとに暗号化し、該暗号化された情報により前記遠隔ファイルのアクセス要求を行い、遠隔ファイルアクセス処理手段は、遠隔ファイルアクセス要求先のコンピュータシステムは、前記遠隔ファイルのアクセス要求を自コンピュータシステムがもつ情報により復号して利用者識別情報を得て、さらに該利用者識別情報をもとに暗号化されている前記認証済証明書とファイルアクセス要求リストを復号して利用者の認証および遠隔ファイルアクセス許否の処理を行い、相互に認証を行う。

【０００９】

【実施例】以下、図面を参照して本発明の実施例について説明する。

【００１０】図１は、本発明の一実施例である遠隔ファイルアクセスシステムの構成ブロック図である。図１において、複数のコンピュータシステム２～５は通信媒体１に接続されている。コンピュータシステム２は、認証サーバであり、ネットワーク上のユーザ情報を一括管理するユーザ情報データベース管理部２－２とユーザのサービス利用許否を判断するための認証済証明書を発行する認証処理部２－１から構成されており、ユーザ情報およびユーザがネットワーク上で利用可能なサービス情報を管理するユーザ情報データベース２－３および暗号鍵データベース２－４が接続されている。コンピュータシステム３～５は、ユーザが一般に利用するコンピュータシステムであり、ユーザ名およびパスワードのユーザ情報を入力する認証要求部３－１～５－１と、他のコンピュータシステムへサービスを要求する遠隔ファイルアクセス要求部３－２～５－２と、他のコンピュータシステムからのサービス要求を受け付ける遠隔ファイルアクセス処理部３－３～５－３から構成される。なお、遠隔ファイルアクセス処理部３－３～５－３は、ファイルシステム６～８のアクセス許可リストを有している。

【００１１】図２は、遠隔ファイルアクセスの概要フローチャートである。図２において、まず、コンピュータシステム３～５の認証要求部３－１～５－１は、ユーザが入力したユーザ名・パスワードをもとに、認証サーバ２の認証処理部２－１にユーザの身元確認を要求し、正しいと判断されて認証済証明書が発行されることにより、ユーザの利用開始手続が完了する（ステップ２１）。次に、この認証済証明書は、コンピュータシステム３～５に保存される。コンピュータシステム３～５の遠隔ファイルアクセス要求部３－２～５－２は、認証済証明書をもとに遠隔ファイルアクセスの要求を行う（ステップ２２）。これに対し、コンピュータシステム３～５の遠隔ファイルアクセス処理部３－３～３－５は、遠隔ファイルアクセス要求のファイルアクセス可否のチェックを行い（ステップ２３）、アクセス許可である場合には、認証済証明書を確認してファイルアクセスが行われる。

【００１２】図３は、認証済証明書のフォーマット図である。図３において、認証済証明書は、認証サーバのホスト名および認証サーバの位置を示すアドレスが格納されている。その他、ユーザ名、ユーザの識別を示すユーザＩＤ番号、認証済証明書の発行時刻および有効期限が格納される。この認証済証明書をもとに、コンピュータシステムの遠隔ファイルアクセス要求部は、遠隔ファイルアクセスを行うことになる

次に、認証済証明書を発行されたコンピュータシステム３のユーザがコンピュータシステム４のファイルアクセスを要求する場合を説明する。この遠隔ファイルアクセス要求は、コンピュータシステム３の遠隔ファイルアクセス要求部３－２が、アクセス要求パケットを組み立てて、該当ノードであるコンピュータシステム４の遠隔ファイルアクセス処理部４－３に転送することによって行われる。

【００１３】図４は、アクセス要求パケットの構成を示す図である。図４において、斜線部４１の認証済証明書とアクセス要求リストは、コンピュータシステム３の要求ユーザの復号鍵で暗号化され、斜線部４０のように、アクセス要求パケット全体は、遠隔ノードであるコンピュータシステム４の暗号鍵で暗号化されている。なお、アクセス要求リストは、対象ファイル名とアクセスの種類が含まれている。

【００１４】図５は、遠隔ファイルアクセス要求部の動作フローチャートである。図５において、まず、認証済証明書を認証サーバ２から受け取ると、コンピュータシステム３の遠隔ファイルアクセス要求部３－２は、遠隔ノードのコンピュータシステム４の遠隔ファイルのアクセス要求リストを作成する（ステップ５１）。次に、ファイルアクセスする遠隔ノードの暗号鍵を取得する（ステップ５２）。さらに、受け取った認証済証明書と作成したアクセス要求リストを、ユーザの身元保証を行うため、ユーザのみが知る復号鍵で暗号化する（ステップ５３）。さらに、ユーザ名、ユーザＩＤ、ステップ５３で暗号化した情報からアクセス要求パケットを作成する（ステップ５４）。その後、遠隔ノードの暗号鍵で暗号化する（ステップ５５）。ここで、この暗号鍵は、認証サーバ２の暗号鍵データベース２－４から取得する。その後、遠隔ノードの遠隔ファイルアクセス処理部に送信する（ステップ５６）。

【００１５】図６は、遠隔ファイルアクセス処理部の動作フローチャートである。図６において、まず、コンピュータシステム４の遠隔ファイルアクセス処理部４－３は、受信したアクセス要求パケットを自己のみが知る復号鍵で復号する（ステップ６１）。次に、アクセス要求

5

パケットが復号できたか否かを判定し（ステップ６２）、復号できない場合は、ステップ６９へ移行し、他のノードへの要求またはネットワーク上第三者によってデータが介在されたと判断して、遠隔ファイルアクセスの処理を否定し、中止する（ステップ６９）。一方、復号できた場合は、アクセス要求パケットの中から、アクセス要求元のユーザ名を取り出し、このユーザ名により認証サーバ２の暗号鍵データベース２－４からユーザの暗号鍵を取得する（ステップ６３）。さらに、この取得された暗号鍵により、アクセス要求リストを復号化する（ステップ６４）。次に、アクセス要求リストが復号できたか否かを判定する（ステップ６５）。復号できない場合は、アクセス要求リストがアクセス要求者のみが知るアクセス要求者の復号鍵で暗号化されているので、異なるユーザからのアクセス要求であるか、第三者により介在されたとしてアクセス要求を否定し、遠隔ファイルアクセス処理を中止する（ステップ６９）。一方、アクセス要求リストが復号された場合は、アクセス要求リストの中から認証済証明書を取り出し、認証済証明書に含まれる認証済証明書の発行時刻と有効期限により、認証済証明書の正当性を判定する（ステップ６６）。認証済証明書の正当性が確認されない場合は、ステップ５５と同様に、遠隔ファイルアクセス処理を否定し、処理を中止する（ステップ６９）。一方、認証済証明書が正当で

6

あると確認できた場合は、さらに、アクセス要求をユーザ識別子（ユーザＩＤ）と遠隔ファイルアクセス処理部４－３が有するアクセス許可リストにより、ファイルアクセスの許可を判断する（ステップ６７）。アクセス許可リストにユーザＩＤでのアクセス許可が登録されていない場合には、ステップ６６と同様に、ファイルアクセスが否定され、アクセス処理が中止される（ステップ６９）。一方、アクセス許可が登録されている場合に、初めて、ファイルアクセスが許可される（ステップ６８）。

【００１６】ここで、ステップ６６における認証済証明書の正当性判断について、詳細に説明する。図７は、認証済証明書の正当性判断フローチャートである。図７において、まず、認証済証明書の中からユーザ名、ユーザＩＤを取り出し（ステップ７１）、ファイルアクセス要求パケットのユーザ名、ユーザＩＤと等しいか否かを判断する（ステップ７２）。ここで、等しくない場合は、不正な認証済証明書として処理される（ステップ７６）。一方、ユーザ名、ユーザＩＤが等しい場合は、現在時刻Ｔｃ、発行時刻Ｔｔ、有効期限Ｔｌを取り出す（ステップ７３）。次に、式（１）が成立するか否かを判断する（ステップ７４）。

【００１７】

$$\text{発行時刻}Tt \leq \text{現在時刻}Tc \leq \text{発行時刻}Tt + \text{有効期限}Tl \qquad (1)$$

次に、式（１）が成立する場合は、正当な認証済証明書として処理し（ステップ７５）、式（２）が成立しない場合は、不正な認証済証明書として処理する（ステップ７６）。

【００１８】なお、以上の実施例においては、公開鍵暗号方式による遠隔ファイルアクセスシステムの例を示しているが、公開鍵暗号方式に限定するものではなく、システムとして最も適する暗号方式を採用すればよい。

【００１９】このようにして、遠隔ファイルアクセスのファイルアクセス権のチェックは、認証証明書を用いて、アクセス要求者が、本来使用すべきユーザＩＤによりアクセス要求を行っているかの判断が可能となり、これによる身元保証を行った上で、ユーザＩＤとファイルアクセスリストによるアクセスチェックを行うため、正確にチェックすることが可能となり、ネットワーク上での遠隔ファイルアクセスシステムの正確性・安全性を向上させることが可能となる。

【００２０】

【発明の効果】以上説明したように、本発明は、複数のコンピュータシステムが任意の通信媒体を介して接続されたネットワーク上で、特定のコンピュータシステムが利用者情報を一括管理して発行する認証済証明書に基づいて、前記複数のコンピュータシステムに接続される遠隔ファイルシステムのファイルアクセスを行う遠隔ファイルアクセスシステムにおいて、遠隔ファイルアクセス要求手段は、遠隔ファイルアクセス要求元のコンピュータシステムは、前記認証済証明書とファイルアクセス要求リストを利用者固有の利用者識別情報をもとに暗号化し、該暗号化された情報と利用者識別情報をさらに前記特定のコンピュータシステムから取得したアクセス要求先コンピュータシステムの情報をもとに暗号化し、該暗号化された情報により前記遠隔ファイルのアクセス要求を行い、遠隔ファイルアクセス処理手段は、遠隔ファイルアクセス要求先のコンピュータシステムは、前記遠隔ファイルのアクセス要求を自コンピュータシステムがもつ情報により復号して利用者識別情報を得て、さらに該利用者識別情報をもとに暗号化されている前記認証済証明書とファイルアクセス要求リストを復号して利用者の認証および遠隔ファイルアクセス許否の処理を行い、相互に認証を行う。すなわち、従来の一方向的なユーザＩＤとアクセス許可リストの組合せによる遠隔ファイルアクセス権のチェックに加えて、アクセス要求者が本来利用するユーザＩＤによって要求しているかを認証することにより、アクセス要求者の身元保証を相互に行うようにしているので、遠隔ファイルシステムのファイルアクセスの正当性・安全性を向上することができるという利点を有する。

【図面の簡単な説明】

【図１】本発明の一実施例である遠隔ファイルアクセスシステムの構成ブロック図。

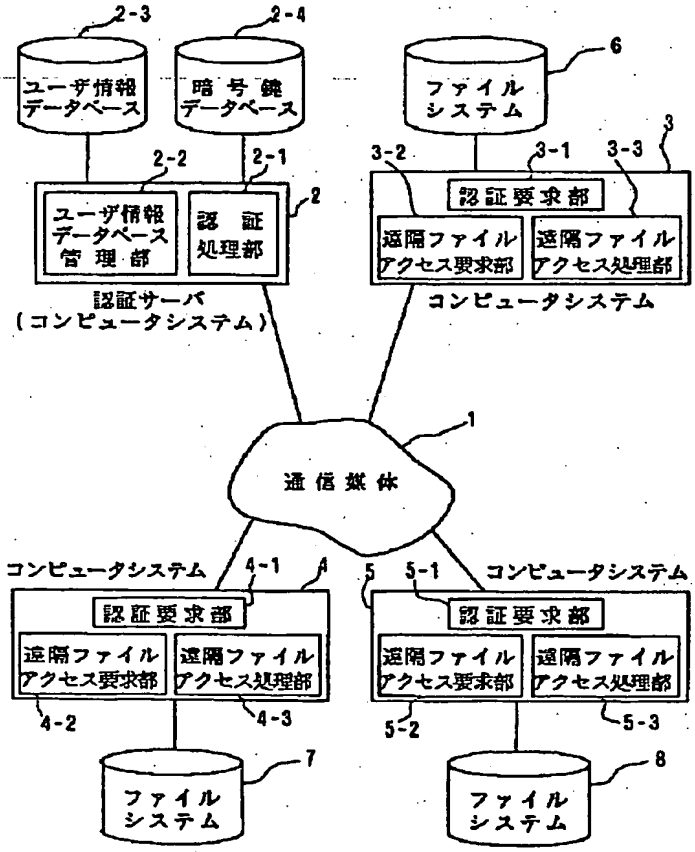
7

【図２】遠隔ファイルアクセスの概要フローチャート。
【図３】認証済証明書のフォーマット図。
【図４】アクセス要求パケットの構成を示す図。
【図５】遠隔ファイルアクセス要求部の動作フローチャート。
【図６】遠隔ファイルアクセス処理部の動作フローチャート。
【図７】認証済証明書の正当性判断フローチャート。
【符号の説明】
1　通信媒体

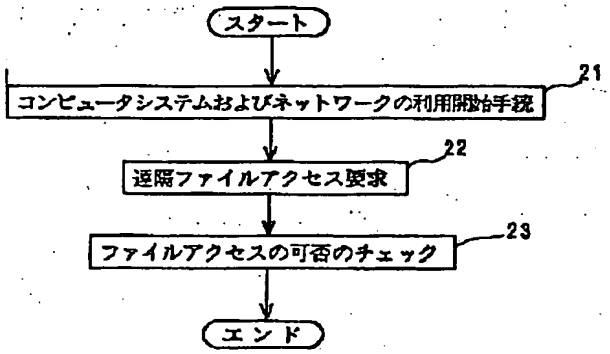
8

2　認証サーバ
2－1　認証処理部
2－2　ユーザ情報データベース管理部
2－3　ユーザ情報データベース
2－4　暗号鍵データベース
3～5　コンピュータシステム
3－1～5－1　認証要求部
3－2～5－2　遠隔ファイルアクセス要求部
3－3～5－3　遠隔ファイルアクセス処理部
6～8　ファイルシステム

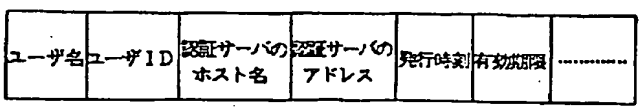
【図１】



【図２】

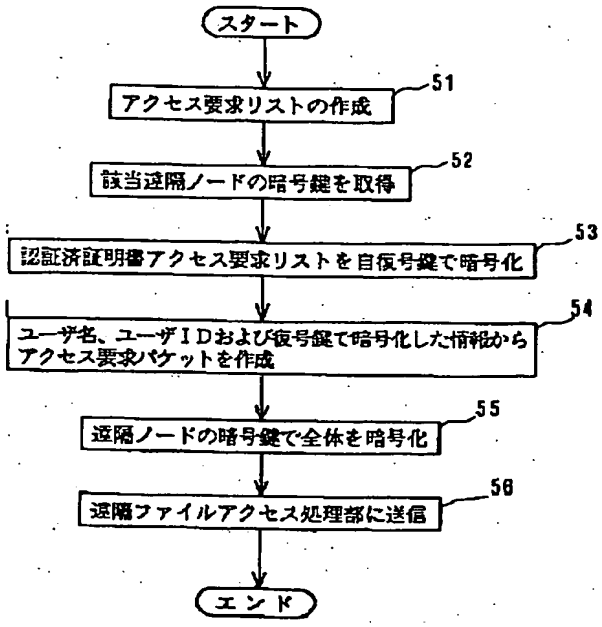


【図３】

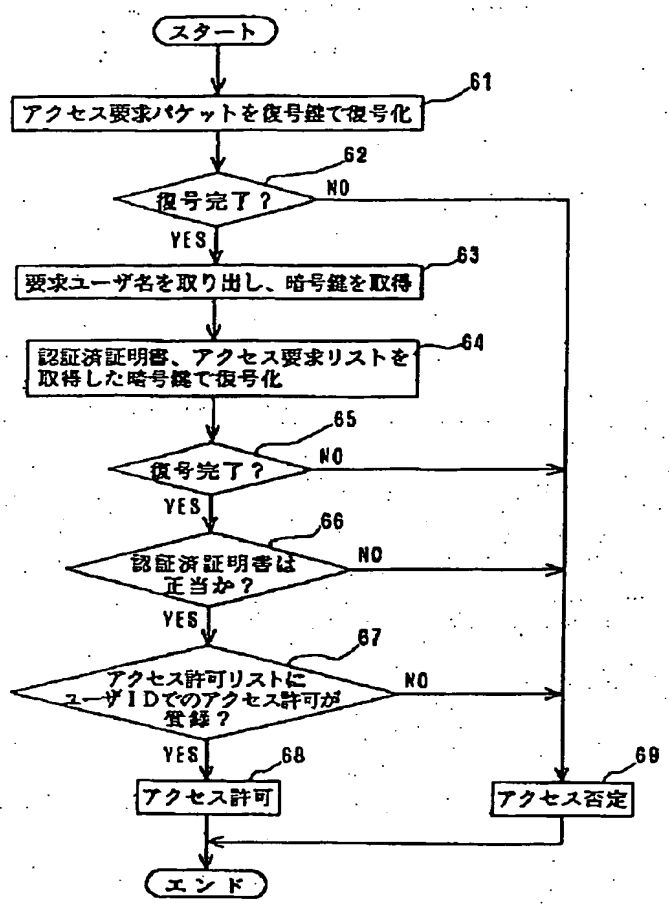


【図４】

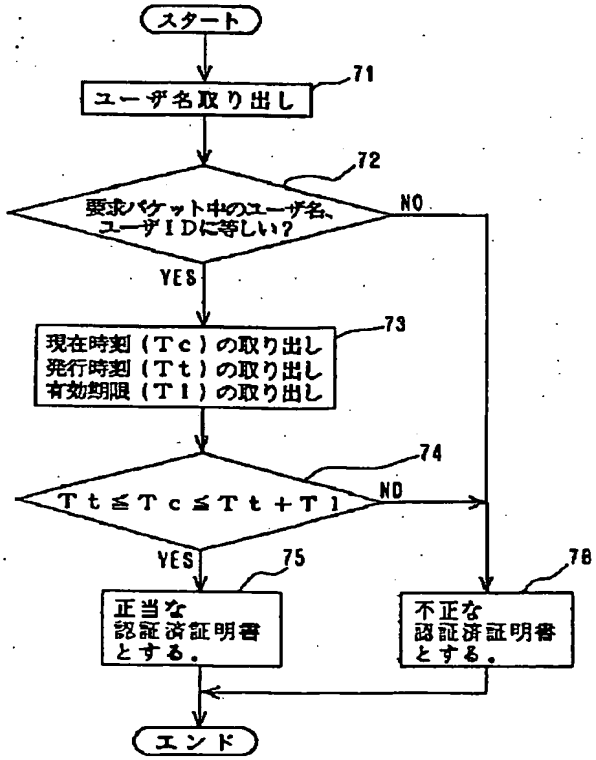
【図５】


スタート
アクセス要求リストの作成
51
該当遠隔ノードの暗号鍵を取得
52
認証済証明書アクセス要求リストを自復号鍵で暗号化
53
ユーザ名、ユーザＩＤおよび復号鍵で暗号化した情報から
アクセス要求パケットを作成
54
遠隔ノードの暗号鍵で全体を暗号化
55
遠隔ファイルアクセス処理部に送信
56
エンド

【図６】


スタート
アクセス要求パケットを復号鍵で復号化
61
復号完了？
62
NO
YES
要求ユーザ名を取り出し、暗号鍵を取得
63
認証済証明書、アクセス要求リストを
取得した暗号鍵で復号化
64
復号完了？
65
NO
YES
認証済証明書は
正当か？
66
NO
YES
アクセス許可リストに
ユーザＩＤでのアクセス許可が
登録？
67
NO
YES
アクセス許可
68
アクセス否定
69
エンド

【図７】


スタート
ユーザ名取り出し
71
要求パケット中のユーザ名、
ユーザＩＤに等しい？
72
NO
YES
現在時刻（Ｔｃ）の取り出し
発行時刻（Ｔｔ）の取り出し
有効期限（Ｔｌ）の取り出し
73
Ｔｔ≦Ｔｃ≦Ｔｔ＋Ｔｌ
74
NO
YES
正当な
認証済証明書
とする。
75
不正な
認証済証明書
とする。
76
エンド